

## SARBANES-OXLEY COMPLIANCE

# SARBANES-OXLEY: ACHIEVING COMPLIANCE BY STARTING WITH ISO 17799

Dwight A. Haworth and Leah R. Pietron

Compliance with the Sarbanes-Oxley Act of 2002 (SOX) has been hampered by the lack of implementation details. This article argues that IT departments that have implemented ten categories of IT controls provided by the International Standards Organization (ISO 17799) will be well on their way toward SOX compliance. A side-by-side comparison of the 124 control components of the ISO Standard and the published SOX implementation guidelines is provided.

**DWIGHT A. HAWORTH** received his B.S. degree from the United States Air Force Academy, Colorado, in 1963. He received his Ph.D. in management information systems from Texas Tech University, Lubbock, Texas, in 1990. He retired from the U.S. Air Force in 1981.

**LEAH R. PIETRON** received her B.S. from Mayville State College, M.S. and Ph.D. from the University of North Dakota, and M.B.A. from Northwest Missouri State University.

**T**HE CONGRESS OF THE UNITED STATES passed the Sarbanes-Oxley Act of 2002 (SOX) in response to financial fraud and deception in firms such as Enron, whose public auditing firm failed to discover this abuse. The purpose of the Act is to prevent these kinds of problems in publicly traded organizations and their business partners, by ensuring that:

- senior management be actively involved with and accountable for the accuracy of the data used in financial reporting, and
- public auditors remain independent of their client firms.

Because the data used in financial reporting is captured, verified, stored, and reported mainly by computer-based systems, senior management has turned to computer security officers to implement the needed controls on those systems.

The Act has been the source of much concern, at least in part because it lacks specifics and in part because implementation details are left to a board created by the Act. The board's implementation guidelines were published in

2003 (Hardesty, 2003, pp. 3005-3011). Lacking specifics, many firms have turned to their external auditors for guidance. Yet when industry groups meet and the subject of Sarbanes-Oxley compliance comes up, participants are sometimes amazed at the variance in the answers each has received. As a result, security officers and others charged with information assurance continue to examine what they must do beyond the measures already in place.

In-place procedures range from those dictated by common sense to those implemented to achieve some formal certification, such as compliance with ISO 17799: *International Standard ISO/IEC 17799 Information Technology — Code of practice for information security management*. Thus, one of the questions being asked is, "How does ISO 17799 relate to SOX?"

The purpose of this study is to describe the relationship of ISO 17799 to the Sarbanes-Oxley Act of 2002. A brief discussion of the provisions of the Act that relate to information technology is first presented. Next, the significant portions of the Public Company Accounting Oversight Board's Audit Standard No. 2 are

**T**he Act and the audit requirements that follow from it are concerned equally with manual and computer-based controls.

highlighted. Finally, the relationships among the elements of ISO 17799, SOX, and Audit Standard No. 2 are discussed in detail, and conclusions are drawn about the relevance of ISO 17799 compliance to a firm seeking compliance with SOX.

### SOX IN A NUTSHELL

The Act itself is simple to follow: parts of the Act deal with external auditors and their relations with clients, other parts mandate additional oversight of auditing and financial reports, and others address issues specific to investment companies. The sections of the Act that are most likely to be of concern to IT departments are discussed here.

### Management Control

A principal objective of the Act is to ensure that a firm's top managers institute controls and are responsible for the operation of those controls. The Act is concerned with controls over the financial data that makes up the required periodic financial reports and other reports required by the U.S. Securities and Exchange Commission (SEC), as well as controls that reveal situations the SEC requires to be reported, such as fraud, embezzlement, and material changes in the operation of the company.

### Systems or Processes

Generalizing from a specific SEC definition (Hardesty, 2003, p. 4051), we interpret a control as a process or procedure designed to achieve a goal. The Act does not mention the mode of implementation. The control may be in the procedure a clerk follows to fill an order, or it may be a complex edit-check of data that is input to a computer program. The Act and the audit requirements that follow from it are concerned equally with manual and computer-based controls.

### Evaluation

Under Sections 302 and 404 of the Act, management is required to assess and report the effectiveness of its internal controls (Hardesty, 2003, pp. 3026, 3035). Furthermore, each public accounting firm that prepares an independent audit of a financial report must also attest to the management's assessment of its internal controls over financial reporting (Hardesty, 2003, p. 3036). The nature of management's assessment is not spelled out, but the Public Company Accounting Oversight Board (PCAOB) has

issued Audit Standard No. 2 (AS No. 2) to guide independent auditors in their evaluation of management's controls. Specific directions instruct auditors to conduct a walkthrough of "major classes of transactions" (PCAOB, 2003, para. 79). This would suggest that management follow similar procedures in its assessment, including both manual and automated processes.

### Disclosure Controls

Less publicized, but equally important, is Section 409; this section requires real-time disclosure of "material changes in the financial condition or operations of the issuer ..." (Hardesty, 2003, p. 3037). Events that may be subject to this kind of reporting include acquisitions, mergers, and divestitures. Hardesty (2003, pp. 439-440) presents a long list of such items; it is clear that many of these items would be known first at the upper echelons of management, and the information would and should be disclosed from offline sources. It is also clear that some events may first be reflected in the books and that information systems may be needed to detect and report such occurrences. Likewise, systems may also be needed (if they do not already exist) to detect embezzlement and fraud.

What is suggested here parallels intrusion detection in a network security system. After all of the access control rules are implemented and the software is updated and patched, an intrusion detection system should provide the ability to determine if and when security controls have been bypassed. After the file access rules are implemented, the checks on transactions are coded, and change control is put into place, the disclosure control system should enable the ability to determine if and when controls on financial transactions have been bypassed.

### Internal Controls over Financial Reporting

The principal focus of the Sarbanes-Oxley Act is on the controls over financial reporting. This is made clear in the statements of Section 404. According to this section, management is required to include in its annual report an assessment of its "internal control structure and procedures for financial reporting" (Hardesty, 2003, p. 3035). In addition, this section requires the registered public accounting firm that prepares the audit report for the firm to attest to the management's assessment of its internal controls. This means that the public accounting firm must be able to evaluate the

***It is axiomatic in the data processing world that program and system documentation is outdated, sometimes even before the system is placed in production.***

means by which management arrived at its assessment.

Many of the requirements that flow from this section depend on the actions of the PCAOB, as provided in AS No. 2. However, this standard had not been issued prior to the implementation board's interpretation (i.e., Hardesty 2003). The implications of AS No. 2 are therefore discussed next.

#### **AUDIT STANDARD NO. 2**

Bear in mind that AS No. 2 is guidance for the auditor in evaluating management's assessment of its internal control over financial reporting. The paragraphs discussed here identify areas the auditor is required to investigate. Knowing that the auditor must investigate these areas, the IT department can prepare for the auditor's evaluation by reviewing and documenting controls in these areas and strengthening controls where appropriate. In doing so, the IT department can reduce the possibility of an adverse evaluation and any sanctions that might follow from such an evaluation.

#### **Paragraph 40**

Paragraph 40 outlines items the auditor should review to understand management's assessment of its internal controls. First among these is a list of controls that apply to "significant accounts" and how management selects which controls to assess. The following items from the list are relevant to IT managers because they are likely to be implemented wholly or in part through computer-based processes (PCAOB, 2004, para. 40):

- Controls over initiating, authorizing, recording, processing, and reporting significant accounts . . . .
- Antifraud programs and controls.
- Controls, including information technology general controls, on which other controls are dependent.
- Controls over significant non-routine and nonsystematic transactions . . . .
- Controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; to initiate authorize, record, and process journal entries in the general ledger, and to record recurring and nonrecurring adjustments to the financial statements . . . .

The auditor is concerned with how management selected the controls to be tested and how management evaluated the design effectiveness and operating effectiveness of the controls. Thus, the company should maintain documentation of management's actions in selecting the controls to test, documentation of the design of the controls and management's view of the effectiveness of the design, and documentation of the test results for the auditor's review. It is axiomatic in the data processing world that program and system documentation is outdated, sometimes even before the system is placed in production. The creation and maintenance of this documentation promises to be a significant challenge for some IT departments.

#### **Paragraph 42**

In Paragraph 42, the PCAOB (2004) lays out the components of the documentation the auditor should seek:

- The design of controls over all relevant assertions related to all significant accounts and disclosures in the financial statements. The documentation should include the five components of internal control over financial reporting as discussed in paragraph 49, including the control environment and company-level controls as described in paragraph 53;
- Information about how significant transactions are initiated, authorized, recorded, processed, and reported;
- Sufficient information about the flow of transactions to identify the points at which material misstatements due to error or fraud could occur;
- Controls designed to prevent or detect fraud, including who performs the controls and the related segregation of duties;
- Controls over the period-end financial reporting process;
- Controls over safeguarding of assets; and
- The results of management's testing and evaluation.

In summary, this paragraph states that each control should be documented on the five elements given in Paragraph 49 (see following section). In addition, for significant transactions, there should be beginning-to-end documentation of the flow, and the controls along that flow should be evaluated for weaknesses with respect to errors and fraud. With respect to the end-of-quarter or end-of-year financial reporting processes, similar documentation is implied.

***Inadequate documentation is considered a deficiency in a company's internal control over financial reporting.***

Specific controls for the protection of assets must also be documented, again on the five components in Paragraph 49.

Finally, the results of management's assessment must be documented.

**Paragraph 45**

This paragraph states that inadequate or insufficient documentation of the controls may be evaluated by the external auditor as a deficiency in management's control. This has the effect of mandating documentation that will prove management's assertions about the financial statements and the controls on those financial statements.

**Paragraph 49**

The auditor is charged with understanding the firm's internal control over financial reporting on five components: the Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. Only those aspects that are proximate to IT transaction processes need be documented by the IT function (see Paragraph 42). Other components, particularly the Control Environment, are outside the purview of IT, as are those parts of Risk Assessment, Control Activities, Information and Communication, and Monitoring that are not proximate to IT-enabled processes.

**Paragraph 53**

In general, company-level controls apply across the firm and are not IT specific. However, the company-level controls may be implemented in computer programs and computer procedures or documented separately and specifically for computer-based processing systems. The following are company-level controls (PCAOB, 2004, para. 53):

- Controls within the control environment, including tone at the top, the assignment of authority and responsibility; ... ;
- Management's risk assessment process;
- Centralized processing and controls, including shared service environments;
- Controls to monitor the results of operations;
- Controls to monitor other controls ... ;
- The period-end financial reporting process.

Those controls that are not part of a documented process must be addressed separately. The documentation for IT-enabled processes that contain company-level controls should be updated and the control documentation made

specific (see previous section on Paragraph 42 above). Inadequate documentation is considered a deficiency in a company's internal control over financial reporting. The auditor may rate it as a significant deficiency or a material weakness. In the latter case, the auditor would make an adverse assessment of management's internal control over financial reporting (PCAOB, 2004, para. 175).

**Paragraph 76**

The following constitute the period-end financial reporting process (PCAOB, 2004, para. 76):

- The procedures used to enter transactions totals into the general ledger;
- The procedures used to initiate, authorize, record, and process journal entries in the general ledger;
- Other procedures used to record recurring and nonrecurring adjustments to the annual and quarterly financial statements ... ;
- Procedures for drafting annual and quarterly financial statements and related disclosures.

The auditor is charged with understanding and evaluating these (PCAOB, 2004, para. 77). The period-end financial reporting process is not only a statement to the company's stakeholders, but also the ultimate disclosure control on operational effectiveness. As such, the integrity of the data and the processes must be unblemished. In some firms the period-end financial reports are prepared by accountants using database queries that have been developed outside the purview of IT department professionals and without any formal development method. As such, documentation of these queries requires thorough review and updating before an auditor evaluation.

**Paragraph 80**

"The auditor's walkthroughs should encompass the entire process of initiating, authorizing, recording, processing, and reporting individual transactions and controls for each of the significant processes identified, including controls intended to address the risk of fraud" (PCAOB, 2004, para. 80).

To support the auditor's walkthroughs and to foster a positive evaluation, it is recommended that IT departments implement the ISO/IEC Standard 17799 and the acknowledged security best practices in compliance with the Act. The application of these recommendations must,

however, always be filtered through the needs identified by management's risk assessment.

### ISO SPECIFICS

The first two sections of ISO 17799 deal with the scope of the Standard and with definitions of terms. Beginning with Section 3, the ISO Standard addresses ten areas: Security Policy; Organizational Security; Asset Classification and Control; Personnel Security; Physical and Environmental Security; Communications and Operations Management; Access Control; Systems Development and Maintenance; Business Continuity Management; and Compliance. Each area is decomposed at least two levels, creating a total of 124 components across all ten areas (see Table 1 for details).

Not all of the ISO components are necessary to comply with the Sarbanes-Oxley Act of 2002 because a few do not deal with the integrity of financial reporting. However, most of the 124 components contribute to the "information technology general controls" upon which the controls on financial reporting depend. Therefore, all ten ISO areas, and most of the components of each area, contribute to the ability of the firm to conform to the requirements of the Act.

On the other hand, ISO 17799 (2000, p. 1) contains only recommendations, and firms are free to choose those recommendations that help them conform to the law and regulations. Most of these recommendations are in the form of best practices. Only portions of the compliance section relate to legal requirements (ISO, 2000, p. x), and because ISO 17799 predates the Sarbanes-Oxley Act of 2002, the "legal requirements" that have been included in ISO 17799 do not reflect those imposed by the Act. Therefore, *the elements of ISO 17799 are reviewed here with the requirements of the Act in mind.*

The following sections summarize the relationship of each ISO area to the Act. The far right column in Table 1 provides specific comments about the applicability to SOX for each of the 124 ISO components.

### Security Policy

This section is an example of one area that must be reevaluated in light of the Act. Although considered a best practice prior to the Act, the items in this section are now addressed by the PCAOB and take on aspects of requirements. However, the firm is left with

discretion about the form of the policy document. An information security policy document prepared in accordance with ISO 17799 (2000, pp. 1-2) should contain references to applicable legislation and regulation. Existing documentation must be updated to reflect the Sarbanes-Oxley Act of 2002 as being an item for compliance.

The PCAOB (2002, para. 49) acknowledges that management's risk assessment plays a part in determining the kind and stringency of controls put in place. For ease of reference, the risk assessment documentation should be included in the larger policy document, and any specific policies created to support the Act should be included as well. Refer to Section A.3 of Table 1 for additional comments on the relationship of specific components to the Act.

### Organizational Security

There appears to be nothing in the legislation or the supporting regulations that requires any of the infrastructure components identified in the Standard; however, such components would be evidence of management's effort to establish a "tone at the top." If third parties have access to financial systems, either directly or indirectly, then this item would be pertinent to SOX compliance. Evidence of management's due diligence and control should be provided by the extensive list of recommended contractual terms (ISO, 2000, pp. 6-7). Outsourced functions must be evaluated similarly. Section A.4 of Table 1 elaborates these security components.

### Asset Classification and Control

An inventory of assets is necessary to detect theft and misappropriation and to establish IT general controls. Moreover, the inventory serves as a starting point to develop the more focused documentation needed to identify points of vulnerability. From a vulnerability assessment, a firm can design countermeasures to prevent unauthorized connections to the company's network, through which access might be gained and data modification or fraud perpetrated. It is noted that information classification is used to determine confidentiality precautions rather than integrity precautions, and therefore information classification is not a necessary component for compliance with the Act. Section A.5 of Table 1 reflects these conclusions.

**A**ll ten of the ISO areas, and most of the components of each area, contribute to the ability of the firm to conform to the requirements of the Act.

**TABLE 1** ISO/IEC 17799, Sections A.3 through A.12

ISO/IEC 17799 Sections	Notes
<b>A.3 SECURITY POLICY</b>	
<b>A.3.1 Information security policy</b>	
<b>A.3.1.1</b> <i>Information security policy document</i>	Policy manuals support management's assessment of its controls (PCAOB, 2004, para. 43). Security policies form the basis for both IT general controls (para. 40) and specific controls over financial reporting (para. 40) that are part of integrity assurance component of information security (ISO, 2000, p. viii).
<b>A.3.1.2</b> <i>Review and evaluation</i>	Quarterly internal assessments of the controls, including policies, and annual assessments by outside auditors are required by the Act (Hardesty, 2003, pp. 3026, 3036). There is no specified frequency for review under ISO 17799 (2000, p. 2); therefore, this is a case where the requirements of the Sarbanes-Oxley Act are more stringent than the ISO Standard.
<b>A.4 ORGANIZATIONAL SECURITY</b>	
<b>A.4.1 Information security infrastructure</b>	
<b>A.4.1.1</b> <i>Management information security forum</i>	There appears to be nothing in the legislation or the supporting regulations that require any of these infrastructure items.
<b>A.4.1.2</b> <i>Information security coordination</i>	There appears to be nothing in the legislation or the supporting regulations that require any of these infrastructure items.
<b>A.4.1.3</b> <i>Allocation of information security responsibilities</i>	There appears to be nothing in the legislation or the supporting regulations that require any of these infrastructure items.
<b>A.4.1.4</b> <i>Authorization process for information processing facilities</i>	No bearing on the focus or intent of the Act.
<b>A.4.1.5</b> <i>Specialist information security advice</i>	No bearing on the focus or intent of the Act.
<b>A.4.1.6</b> <i>Cooperation between organizations</i>	No bearing on the focus or intent of the Act.
<b>A.4.1.7</b> <i>Independent review of information security</i>	For those items that are common to ISO 17799 and SOX, the ISO requirement for review and evaluation will probably be satisfied by the annual outside auditor evaluation of management's assessment of its internal controls.
<b>A.4.2 Security of third-party access</b>	
<b>A.4.2.1</b> <i>Identification of risks from third-party access</i>	The entire risk assessment process is one of the factors that the auditor must evaluate according to the PCAOB (2004, para. 49). If third parties have access to financial systems, either directly or indirectly, then this item would be pertinent to SOX compliance.
<b>A.4.2.2</b> <i>Security requirements in third-party contracts</i>	This is one component of IT general controls specified by the PCAOB (2004, para. 50).
<b>A.4.3 Outsourcing</b>	
<b>A.4.3.1</b> <i>Security requirements in outsourcing contracts</i>	It is noted that the ISO neglected to include a risk assessment component under this section but included risk assessment for third-party access. It is assumed that this is a mere oversight and that risk assessment would be a best practice for outsourcing contracts. For completeness, all outsourcing contracts should be evaluated for risks, and security requirements should be included in those contracts where appropriate. This would satisfy paragraphs 49 and 50 of AS No. 2 (PCAOB, 2004). The list of contractual terms under third-party access is recommended for outsourcing contracts (ISO, 2000, p. 8).
<b>A.5 ASSET CLASSIFICATION AND CONTROL</b>	
<b>A.5.1 Accountability for assets</b>	
<b>A.5.1.1</b> <i>Inventory of assets</i>	First step to prevent misappropriation of company assets, which is a requirement under AS No. 2, para. 24. The inventory of assets becomes part of the IT general controls listed in Paragraph 40 (PCAOB, 2004).

**TABLE 1** ISO/IEC 17799, Sections A.3 through A.12 (Continued)

ISO/IEC 17799 Sections	Notes
<b>A.5.2 Information classification</b>	
<b>A.5.2.1</b> <i>Classification guidelines</i>	Classification does not seem to have a bearing on data integrity, the primary concern of the Act, and therefore is not relevant to compliance with the Act.
<b>A.5.2.2</b> <i>Information labeling and handling</i>	Labeling does not seem to have a bearing on data integrity, the primary concern of the Act, and therefore is not relevant to compliance with the Act.
<b>A.6 PERSONNEL SECURITY</b>	
<b>A.6.1 Security in job definition and resourcing</b>	
<b>A.6.1.1</b> <i>Including security in job responsibilities</i>	One component of the general controls that provide foundation for more specific controls as described in Paragraphs 40 and 50 (PCAOB, 2004). Such a practice may also be viewed as a significant part of the control environment discussed in Paragraph 53 (PCAOB, 2004).
<b>A.6.1.2</b> <i>Personnel screening and policy</i>	Such practices are a significant part of the general controls of Paragraphs 40 and 50; they may also be regarded as a specific control to prevent fraud, thus satisfying in part the requirements of Paragraphs 25 and 40 (PCAOB, 2004).
<b>A.6.1.3</b> <i>Confidentiality agreements</i>	The use or non-use of <i>confidentiality agreements</i> does not have a direct bearing on the provisions of the Act nor on any of the provisions of AS No. 2 (PCAOB, 2004).
<b>A.6.1.4</b> <i>Terms and conditions of employment</i>	<i>Terms and conditions of employment</i> , when coupled with security in job responsibilities (above), can be a major part of the control environment of Paragraph 53 (PCAOB, 2004).
<b>A.6.2 User training</b>	
<b>A.6.2.1</b> <i>Information security education and training</i>	An <i>information security education and training</i> program serves as evidence of the strength of the control environment and the "tone at the top" that is the subject of Paragraph 40. Such a program is also part of the "information technology general controls" that are to be included in the evaluation of management's assessment prescribed by Paragraph 53 (PCAOB, 2004).
<b>A.6.3 Responding to security incidents and malfunctions</b>	
<b>A.6.3.1</b> <i>Reporting security incidents</i>	A detective control and possibly the last line of preventive control in the right circumstances. Such reporting may be used as input to management's assessment of its controls. Such measures would fall into the category of controls to monitor other controls listed under company-level controls in Paragraph 53 (PCAOB, 2004).
<b>A.6.3.2</b> <i>Reporting security weaknesses</i>	A detective control and possibly the last line of preventive control in the right circumstances. Such reporting may be used as input to management's assessment of its controls. Such measures would fall into the category of controls to monitor other controls listed under company-level controls in Paragraph 53 (PCAOB, 2004).
<b>A.6.3.3</b> <i>Reporting software malfunctions</i>	A detective control and possibly the last line of preventive control in the right circumstances. Such reporting may be used as input to management's assessment of its controls. Such measures would fall into the category of controls to monitor other controls listed under company-level controls in Paragraph 53 (PCAOB, 2004).
<b>A.6.3.4</b> <i>Learning from incidents</i>	Part of management's ongoing risk assessment and the basis for identifying improved controls.
<b>A.6.3.5</b> <i>Disciplinary process</i>	Evidence of management's effort to set the "tone at the top," as well as being good management practice.
<b>A.7 PHYSICAL AND ENVIRONMENTAL SECURITY</b>	
<b>A.7.1 Secure areas</b>	
<b>A.7.1.1</b> <i>Physical security perimeter</i>	All controls are components of IT general controls (PCAOB, 2004, para. 50).
<b>A.7.1.2</b> <i>Physical entry controls</i>	All controls are components of IT general controls (PCAOB, 2004, para. 50).
<b>A.7.1.3</b> <i>Securing offices, rooms and facilities</i>	All controls are components of IT general controls (PCAOB, 2004, para. 50).
<b>A.7.1.4</b> <i>Working in secure areas</i>	All controls are components of IT general controls (PCAOB, 2004, para. 50).



**TABLE 1** ISO/IEC 17799, Sections A.3 through A.12 (Continued)

ISO/IEC 17799 Sections	Notes
<b>A.7.1.5</b> <i>Isolated delivery and loading areas</i>	Contributes to the security of inbound and outbound merchandise and equipment and is a company-level control (PCAOB, 2004, para. 53).
<b>A.7.2 Equipment security</b>	
<b>A.7.2.1</b> <i>Equipment setting and protection</i>	The Act requires management to report on controls that are designed to support the issuer's "ability to record, process, summarize and report financial data ..." with the emphasis on the word "ability" (Hardesty, 2004, p. 3027).
<b>A.7.2.2</b> <i>Power supplies — Equipment shall be protected from power failures and other electrical anomalies</i>	The Act requires management to report on controls that are designed to support the issuer's "ability to record, process, summarize and report financial data ..." with the emphasis on the word "ability" (Hardesty, 2004, p. 3027).
<b>A.7.2.3</b> <i>Cabling security</i>	The security of data cables against surreptitious connections is important as control against insertion of fraudulent data into data streams.
<b>A.7.2.4</b> <i>Equipment maintenance</i>	The Act requires management to report on controls that are designed to support the issuer's "ability to record, process, summarize and report financial data ..." with the emphasis on the word "ability" (Hardesty, 2004, p. 3027).
<b>A.7.2.5</b> <i>Security of equipment off-premises</i>	Is a SOX relevant issue to the extent that the equipment that is off premises may be used to gain access to the financial processing systems or to the financial data directly.
<b>A.7.2.6</b> <i>Secure disposal or re-use of equipment</i>	Relevant to protecting access and integrity controls if the equipment contains information that could be used to circumvent those controls.
<b>A.7.3 General controls</b>	
<b>A.7.3.1</b> <i>Clear desk and clear screen policy</i>	The <i>clear desk and clear screen policy</i> falls into the IT general controls of AS No. 2, Paragraph 50 (PCAOB, 2004).
<b>A.7.3.2</b> <i>Removal of property</i>	May be relevant to protecting financial data integrity controls if the property contains information that could be used to circumvent those controls; such controls are necessary in preventing misappropriation of company assets which is covered by AS No. 2, Paragraph 24 (PCAOB, 2004).
<b>A.8 COMMUNICATIONS AND OPERATIONS MANAGEMENT</b>	
<b>A.8.1 Operational procedures and responsibilities</b>	
<b>A.8.1.1</b> <i>Documented operating procedures</i>	The operating procedures contain directions for processing financial data, the operating procedures become part of management's documentation addressed in AS No. 2, Paragraphs 42 and 43 (PCAOB, 2004).
<b>A.8.1.2</b> <i>Operational change controls</i>	Is specifically mentioned in Paragraph 50 as being part of the IT general controls (PCAOB, 2004).
<b>A.8.1.3</b> <i>Incident management procedures</i>	Covers procedures for dealing with processing errors and fraudulent entries that fall under the scope of the legislation and AS No. 2, Paragraph 49 (PCAOB, 2004). The multiple aspects of these procedures described in the ISO Standard make incident management procedures a key component for detection and recovery from errors and frauds (International Organization for Standardization, 2000, pp. 20–21).
<b>A.8.1.4</b> <i>Segregation of duties</i>	Should be planned with a view to preventing fraud and other security failures according to the ISO Standard (International Organization for Standardization, 2000, p. 21). Segregation of duties is specifically identified as a part of management's documentation of controls (PCAOB, 2004, para. 42).
<b>A.8.1.5</b> <i>Separation of development and operational facilities</i>	This is one more component of IT general controls (PCAOB, 2004, para. 50). It is a specific control to prevent accidental corruption of financial data during development and testing.
<b>A.8.1.6</b> <i>External facilities management</i>	May be an issue under the Act and AS No. 2 if financial data processing is outsourced. Should such outsourcing be done, all controls necessary to assure the integrity of that financial data must be applied.
<b>A.8.2 System planning and acceptance</b>	
<b>A.8.2.1</b> <i>Capacity planning</i>	This control is a component of compliance with the Act because the Act requires management to report on controls that are designed to support the issuer's "ability to record, process, summarize and report financial data ..." with the emphasis on the word "ability" (Hardesty, 2004, p. 3027).



**TABLE 1** ISO/IEC 17799, Sections A.3 through A.12 (Continued)

ISO/IEC 17799 Sections	Notes
<b>A.8.2.2</b> <i>System acceptance</i>	Another component of IT general controls (PCAOB, 2004, para. 50). Testing must cover the range of controls designed to preserve the integrity of that data, and that testing would be part of compliance with AS No.2, Paragraph 40 (PCAOB, 2004).
<b>A.8.3 Protection against malicious software</b>	
<b>A.8.3.1</b> <i>Controls against malicious software</i>	The Act requires management to report on controls that are designed to support the issuer's "ability to record, process, summarize and report financial data ..." with the emphasis on the word "ability" (Hardesty, 2004, p. 3027).
<b>A.8.4 Housekeeping</b>	
<b>A.8.4.1</b> <i>Information back-up</i>	Another of the controls designed to support the issuer's "ability to record, process, summarize and report financial data ..." (Hardesty, 2004, p. 3027). Backups also may be used to detect data integrity failures through comparison and reconciliation programs; thus backups may be a control activity in accordance with Paragraph 49 (PCAOB, 2004).
<b>A.8.4.2</b> <i>Operator logs</i>	An IT general control, and may be a specific control to detect failures related to data integrity and therefore be control activities in accordance with Paragraph 49 (PCAOB, 2004).
<b>A.8.4.3</b> <i>Fault logging</i>	An IT general control, and may be a specific control to detect failures related to data integrity and therefore be control activities in accordance with Paragraph 49 (PCAOB, 2004).
<b>A.8.5 Network management</b>	
<b>A.8.5.1</b> <i>Network controls</i>	Another in the category of IT general controls (PCAOB, 2004, para. 50). Some network controls may be specific controls to prevent or detect compromises of data integrity in accordance with Paragraph 49 (PCAOB, 2004).
<b>A.8.6 Media handling and security</b>	
<b>A.8.6.1</b> <i>Management of removable computer media</i>	As controls to prevent reconnaissance by someone intent on fraud or denial of service, they become items of the IT general controls (PCAOB, 2004, para. 50).
<b>A.8.6.2</b> <i>Disposal of media</i>	As controls to prevent reconnaissance by someone intent on fraud or denial of service, they become items of the IT general controls (PCAOB, 2004, para. 50).
<b>A.8.6.3</b> <i>Information handling procedures</i>	As controls to prevent reconnaissance by someone intent on fraud or denial of service, they become items of the IT general controls (PCAOB, 2004, para. 50).
<b>A.8.6.4</b> <i>Security of system documentation</i>	As controls to prevent reconnaissance by someone intent on fraud or denial of service, they become items of the IT general controls (PCAOB, 2004, para. 50).
<b>A.8.7 Exchanges of information and software</b>	
<b>A.8.7.1</b> <i>Information and software exchange agreements</i>	Such agreements are components of IT general controls specified in Paragraph 50; such agreements may also contain specific controls to prevent or detect compromises of data integrity in accordance with Paragraph 49 (PCAOB, 2004).
<b>A.8.7.2</b> <i>Security of media in transit</i>	Such controls are part of IT general controls; however, specific controls to prevent/detect compromises of data integrity are mandated by Paragraph 49 (PCAOB, 2004).
<b>A.8.7.3</b> <i>Electronic commerce security</i>	These controls are required in accordance with Paragraph 49 (PCAOB, 2004). A significant issue may be nonrepudiation controls to ensure the authenticity of the source of transactions. Moreover, these controls must be documented so as to support the auditor's walkthrough that is required by Paragraph 80 (PCAOB, 2004).
<b>A.8.7.4</b> <i>Security of electronic mail</i>	Over and above the general controls, specific controls to preserve and protect whistleblower communications may be required as part of the disclosure controls mandated by Section 302 (a)(4)(a) (Hardesty, 2003, p. 3026).
<b>A.8.7.5</b> <i>Security of electronic office systems</i>	These controls are components of IT general controls described in Paragraph 50 (PCAOB, 2004). To the degree that any of these systems are used to record, process, or summarize financial data, they become subject to controls required by the Act and Paragraph 49 (PCAOB, 2004).
<b>A.8.7.6</b> <i>Publicly available systems</i>	These controls are components of IT general controls described in Paragraph 50 (PCAOB, 2004). To the degree that any of these systems are used to record, process, or summarize financial data they become subject to controls required by the Act and Paragraph 49 (PCAOB, 2004).

**TABLE 1** ISO/IEC 17799, Sections A.3 through A.12 (Continued)

ISO/IEC 17799 Sections	Notes
<b>A.8.7.7</b> <i>Other forms of information exchange</i>	These controls are components of IT general controls described in Paragraph 50 (PCAOB, 2004). To the degree other forms of information exchange are used to initiate, record, process, or summarize financial data, they become subject to controls required by the Act and Paragraph 49 (PCAOB, 2004).
<b>A.9 ACCESS CONTROL</b>	
<b>A.9.1 Business requirement for access control</b>	
<b>A.9.1.1</b> <i>Access control policy</i>	Policy manuals are identified in Paragraph 43 as a form of management documentation used as a basis for the auditor's evaluation (PCAOB, 2004). Under Paragraph 43, access control policy should address all of the elements outlined in Paragraph 49 (PCAOB, 2004). Security policies form the basis for both IT general controls and specific controls over financial reporting that are part of integrity assurance component of information security (ISO, 2000, p. viii).
<b>A.9.2 User access management</b>	
<b>A.9.2.1</b> <i>User registration</i>	User registration is a component of IT controls upon which other controls depend (PCAOB, 2004, para. 50).
<b>A.9.2.2</b> <i>Privilege management</i>	Privilege management is a component of IT controls upon which other controls depend (PCAOB, 2004, para. 50).
<b>A.9.2.3</b> <i>User password management</i>	User password management is a component of IT controls upon which other controls depend (PCAOB, 2004, para. 50).
<b>A.9.2.4</b> <i>Review of user access rights</i>	Review of user access rights is a component of IT controls upon which other controls depend (PCAOB, 2004, para. 50).
<b>A.9.3 User responsibilities</b>	
<b>A.9.3.1</b> <i>Password use</i>	Policies on password use are components of IT general controls (PCAOB, 2004, para. 50). These policies, when enforced and coupled with system logs of user activity, become a key control to prevent surreptitious access and fraud in electronically processed data.
<b>A.9.3.2</b> <i>Unattended user equipment</i>	Policies on unattended user equipment are components of IT general controls (PCAOB, 2004, para. 50). These policies, when enforced and coupled with system logs of user activity, become a key control to prevent surreptitious access and fraud in electronically processed data.
<b>A.9.4 Network access control</b>	
<b>A.9.4.1</b> <i>Policy on use of network services</i>	Such a policy forms the basis for both IT general controls (PCAOB, 2004, para. 50) and specific controls over financial reporting that are part of integrity assurance component of information security (ISO, 2000, p. viii).
<b>A.9.4.2</b> <i>Enforced path</i>	A control activity under Paragraph 49 (PCAOB, 2004) when it is applied.
<b>A.9.4.3</b> <i>User authentication for external connections</i>	A control activity under Paragraph 49 (PCAOB, 2004). When enforced and coupled with logs of user activity, become a key control to prevent surreptitious access and fraud in electronically processed data.
<b>A.9.4.4</b> <i>Node authentication</i>	A control activity under Paragraph 49 (PCAOB, 2004). Because of the capability to forge source addresses on network packets, authentication on the basis of source node alone is generally not considered a desirable method of authentication.
<b>A.9.4.5</b> <i>Remote diagnostic port protection</i>	One component of IT general controls (PCAOB, 2004, para. 50).
<b>A.9.4.6</b> <i>Segregation in networks</i>	One component of IT general controls (PCAOB, 2004, para. 50). When financial data and financial processing is placed on servers that are segregated in a restricted subnet, segregation may be a significant control to restrict access and preserve the integrity of financial data under Paragraph 49 (PCAOB, 2004).
<b>A.9.4.7</b> <i>Network connection control</i>	One component of IT general controls (PCAOB, 2004, para. 50). It can be a significant control to prevent or restrict access and preserve the integrity of financial data in accordance with Paragraph 49 (PCAOB, 2004).
<b>A.9.4.8</b> <i>Network routing control</i>	One component of IT general controls upon which other security measures depend (PCAOB, 2004, para. 50).
<b>A.9.4.9</b> <i>Security of network services</i>	One component of IT general controls upon which other security measures depend (PCAOB, 2004, para. 50).

**TABLE 1** ISO/IEC 17799, Sections A.3 through A.12 (Continued)

ISO/IEC 17799 Sections	Notes
<b>A.9.5 Operating system access control</b>	
<b>A.9.5.1</b> <i>Automatic terminal identification</i>	May be needed to prevent surreptitious access and fraud in financial data. When implemented, this procedure would be a control under Paragraph 49 (PCAOB, 2004).
<b>A.9.5.2</b> <i>Terminal log-on procedures</i>	Key controls to prevent surreptitious access and fraud in electronically processed data in accordance with Paragraph 49 (PCAOB, 2004).
<b>A.9.5.3</b> <i>User identification and authentication</i>	Key controls to prevent surreptitious access and fraud in electronically processed data in accordance with Paragraph 49 (PCAOB, 2004).
<b>A.9.5.4</b> <i>Password management system</i>	Another component of IT general controls (PCAOB, 2004, para. 50). If user identification and authentication is accomplished by means of passwords, then the password management system is a key element and must be examined very closely for weaknesses because all other integrity measures depend on it.
<b>A.9.5.5</b> <i>Use of system utilities</i>	Restriction on the use of system utilities is another component of IT general controls (PCAOB, 2004, para. 50).
<b>A.9.5.6</b> <i>Duress alarm to safeguard users</i>	The implementation of a duress alarm to safeguard users is not significant to the goals of the Act and is therefore deemed to be beyond the scope of the Act.
<b>A.9.5.7</b> <i>Terminal time-out</i>	A component of IT general controls (PCAOB, 2004, para. 50). It is also an important control to prevent unauthorized access to financial data in accordance with Paragraph 49 (PCAOB, 2004).
<b>A.9.5.8</b> <i>Limitation of connection time</i>	A component of IT general controls (PCAOB, 2004, para. 50). It is also an important control to prevent unauthorized access to financial data in accordance with Paragraph 49 (PCAOB, 2004).
<b>A.9.6 Application access control</b>	
<b>A.9.6.1</b> <i>Information access restriction</i>	A key control to prevent unauthorized access to financial data in accordance with Paragraph 49 (PCAOB, 2004). All of the measures identified in the ISO Standard (ISO, 2000, p. 43) are reasonable and necessary for assuring financial data integrity as envisioned by the Act.
<b>A.9.6.2</b> <i>Sensitive system isolation</i>	May be a necessary measure, depending on management's risk assessment. Should it be deemed necessary, this measure becomes a control under Paragraph 49 (PCAOB, 2004).
<b>A.9.7 Monitoring system access and use</b>	
<b>A.9.7.1</b> <i>Event logging</i>	Needed to detect unauthorized access to financial systems and data and considered a key control activity under Paragraph 49 (PCAOB, 2004).
<b>A.9.7.2</b> <i>Monitoring system use</i>	Includes what risk factors should be considered, what to log, and when to review the logs (ISO, 2000, pp. 44–45). This is a key control activity under Paragraph 49 (PCAOB, 2004).
<b>A.9.7.3</b> <i>Clock synchronization</i>	Another measure that falls into the category of IT general controls (PCAOB, 2004, para. 50).
<b>A.9.8 Mobile computing and teleworking</b>	
<b>A.9.8.1</b> <i>Mobile computing</i>	A component of the IT general controls of Paragraph 50 (PCAOB, 2004). Specific issues and controls and particular concerns are expressed regarding unauthorized remote access to systems (ISO, 2002, pp. 46–47). Each of these may become a control activity under Paragraph 49 (PCAOB, 2004) if access to financial data is available or financial processing is performed using these remote technologies.
<b>A.9.8.2</b> <i>Teleworking</i>	A component of the IT general controls of Paragraph 50 (PCAOB, 2004). ISO provides some details about specific issues and controls, and particular concerns are expressed regarding unauthorized remote access to systems (ISO, 2002, pp. 46–47). Each of these may become a control activity under Paragraph 49 (PCAOB, 2004) if access to financial data is available or financial processing is performed using these remote technologies.
<b>A.10 SYSTEMS DEVELOPMENT AND MAINTENANCE</b>	
<b>A.10.1 Security requirements of systems</b>	
<b>A.10.1.1</b> <i>Security requirements analysis and specification</i>	Another of the IT general controls under Paragraph 50 (PCAOB, 2004). Documentation may become part of management's documentation of its internal controls under Paragraph 43 (PCAOB, 2004).

**TABLE 1** ISO/IEC 17799, Sections A.3 through A.12 (Continued)

ISO/IEC 17799 Sections	Notes
<b>A.10.2 Security in application systems</b>	
<b>A.10.2.1</b> <i>Input data validation</i>	A significant consideration and becomes a key control under Paragraph 49 (PCAOB, 2004). Documentation of the manual processes may usually be found in procedure manuals and are part of management's documentation (PCAOB, 2004, para. 43). A firm may arrive at the position in which key controls are in place and operating effectively but for which adequate documentation is unavailable for either management's assessment, Paragraph 43, or the auditor's walkthrough, Paragraph 80 (PCAOB, 2004).
<b>A.10.2.2</b> <i>Control of internal processing</i>	Provides for the special controls that may be needed to ensure processing conforms to GAAP. This is a key control under Paragraph 49 (PCAOB, 2004). Once again the firm may find itself with inadequate documentation as described above.
<b>A.10.2.3</b> <i>Message authentication</i>	To the extent that financial transactions are entered into the system from message traffic, this becomes a key control over financial data under Paragraph 49 (PCAOB, 2004).
<b>A.10.2.4</b> <i>Output data validation</i>	May be needed to ensure outputs are reconciled in accordance with GAAP. As such, this becomes another key control over financial data under Paragraph 49 (PCAOB, 2004).
<b>A.10.3 Cryptographic controls</b>	
<b>A.10.3.1</b> <i>Policy on the use of cryptographic controls</i>	One or more policies that form the basis for both IT general controls and specific controls over financial reporting under Paragraph 40 (PCAOB, 2004). The focus is on the integrity assurance component of information security (ISO, 2000, p. viii). This policy becomes a part of management's documentation under Paragraph 43 and should address all of the elements outlined in Paragraph 49 (PCAOB, 2004).
<b>A.10.3.2</b> <i>Encryption</i>	May be used to ensure data integrity and, if so used, a key control under Paragraph 49 (PCAOB, 2004).
<b>A.10.3.3</b> <i>Digital signatures</i>	May be needed to ensure the integrity of data communicated through open networks and therefore may be a key control under Paragraph 49 (PCAOB, 2004).
<b>A.10.3.4</b> <i>Non-repudiation services</i>	May also be needed to ensure the authenticity of financial transactions communicated through open networks and to screen out fraudulent transactions. Such controls also become key controls under Paragraph 49 (PCAOB, 2004).
<b>A.10.3.5</b> <i>Key management</i>	Needed only if cryptography is used for authentication or integrity controls and becomes one of the IT general controls upon which other controls depend (PCAOB, 2004, para. 50).
<b>A.10.4 Security of system files</b>	
<b>A.10.4.1</b> <i>Control of operational software</i>	One component of IT general controls within the purview of Paragraph 50 (PCAOB, 2004).
<b>A.10.4.2</b> <i>Protection of system test data</i>	A component of IT general controls within the purview of Paragraph 50 (PCAOB, 2004).
<b>A.10.4.3</b> <i>Access control to program source library</i>	One component of IT general controls that is specifically mentioned in Paragraph 50 (PCAOB, 2004).
<b>A.10.5 Security in development and support processes</b>	
<b>A.10.5.1</b> <i>Change control procedures</i>	A component of IT general controls that is specifically mentioned in Paragraph 50 (PCAOB, 2004).
<b>A.10.5.2</b> <i>Technical review of operating system changes</i>	One component of IT general controls under Paragraph 50 (PCAOB, 2004).
<b>A.10.5.3</b> <i>Restrictions on changes to software packages</i>	Another component of IT general controls under Paragraph 50 (PCAOB, 2004).
<b>A.10.5.4</b> <i>Covert channels and Trojan code</i>	Additional security issues, the controls for which are IT general controls under Paragraph 50 (PCAOB, 2004).
<b>A.10.5.5</b> <i>Outsourced software development</i>	Another component of IT general controls under Paragraph 50 (PCAOB, 2004).



**TABLE 1** ISO/IEC 17799, Sections A.3 through A.12 (Continued)

ISO/IEC 17799 Sections	Notes
<b>A.11 BUSINESS CONTINUITY MANAGEMENT</b>	
<b>A.11.1 Aspects of business continuity management</b>	
<b>A.11.1.1</b> <i>Business continuity management process</i>	A component of a continuity of operations plan that may be inferred from the language of the Act in which controls are designed to support the issuer's "ability to record, process, summarize, and report financial data ..." (Hardesty, 2003, p. 3027).
<b>A.11.1.2</b> <i>Business continuity and impact analysis</i>	A component of a continuity of operations planning process that may be inferred from the language of the Act in which controls are designed to support the issuer's "ability to record, process, summarize, and report financial data ..." (Hardesty, 2003, p. 3027).
<b>A.11.1.3</b> <i>Writing and implementing continuity plans</i>	A component of a continuity of operations planning process that may be inferred from the language of the Act in which controls are designed to support the issuer's "ability to record, process, summarize, and report financial data ..." (Hardesty, 2003, p. 3027).
<b>A.11.1.4</b> <i>Business continuity planning framework</i>	An aspect of a continuity of operations planning process that may be inferred from the language of the Act in which controls are designed to support the issuer's "ability to record, process, summarize, and report financial data ..." (Hardesty, 2003, p. 3027).
<b>A.11.1.5</b> <i>Testing, maintaining, and re-assessing business continuity plans</i>	Because the evaluations are tied to periodic financial reports, the Act requires more frequent and more detailed evaluations than the ISO Standard, which has no mention of timing of evaluations.
<b>A.12 COMPLIANCE</b>	
<b>A.12.1 Compliance with legal requirements</b>	
<b>A.12.1.1</b> <i>Identification of applicable legislation</i>	Because of continuing changes in the law and the regulatory environments (the Sarbanes–Oxley Act of 2002 is an example), this must be an ongoing activity.
<b>A.12.1.2</b> <i>Intellectual property rights (IPR)</i>	These areas are covered by existing legislation or legal precedent.
<b>A.12.1.3</b> <i>Safeguarding of organizational records</i>	These areas are covered by existing legislation or legal precedent.
<b>A.12.1.4</b> <i>Data protection and privacy of personal information</i>	These areas are covered by existing legislation or legal precedent; however, recent incidents may motivate additional legislation that may impose stricter requirements.
<b>A.12.1.5</b> <i>Prevention of misuse of information processing facilities</i>	These areas are covered by existing legislation or legal precedent.
<b>A.12.1.6</b> <i>Regulation of cryptographic controls</i>	These areas are covered by existing legislation.
<b>A.12.1.7</b> <i>Collection of evidence</i>	There seems to be no intent in the Act to mandate prosecution of those who commit fraud, only that the fraud be detected and reported (Hardesty, 2003, p. 3027). Therefore, it appears that procedures for the collection of evidence are beyond the scope of the Act.
<b>A.12.2 Reviews of security policy and technical compliance</b>	
<b>A.12.2.1</b> <i>Compliance with security policy</i>	A component that the ISO Standard has in common with the Act and AS No. 2. As with legal compliance (above), the ISO Standard suggests no timing other than "regular reviews" (ISO, 2002, p. 64).
<b>A.12.2.2</b> <i>Technical compliance checking</i>	A component that the ISO Standard has in common with the Act and AS No. 2. As with legal compliance (above), the ISO Standard suggests no timing other than "regular reviews" (ISO, 2002, p. 64).
<b>A.12.3 System audit considerations</b>	
<b>A.12.3.1</b> <i>System audit controls</i>	These form part of the IT general controls and provide one means for management to evaluate the effectiveness of other IT controls (PCAOB, 2004, para. 49).
<b>A.12.3.2</b> <i>Protection of system audit tools</i>	The suite of tools used to audit information systems must be reviewed regularly to ensure coverage of the IT general controls and the specific controls over financial reporting. These appear to fall under the monitoring area of Paragraph 49 (PCAOB, 2004).

**Only careful access control can prevent or detect the recording of fraudulent or erroneous data in significant accounts.**

### **Personnel Security**

The components of this area serve to establish the security environment and may be viewed as management's first line of defense in preventing fraud and embezzlement. Many of the components serve to ensure the honesty and integrity of personnel who will handle financial data and assets, as well as of those who will provide the information technology that will be used to process that data. Only one component, confidentiality agreements, seems to have no bearing on the provisions of the Act or on any of the provisions of AS No. 2 (PCAOB, 2004); however, the use of confidentiality agreements may be viewed as another part of the control environment and the "tone at the top" that is necessary for financial control. Section A.6 in Table 1 comments on the individual components.

### **Physical and Environmental Security**

All components of this area are IT general controls. Further, control of physical access to computer equipment limits access to all systems and data and is therefore a significant control in the protection of financial systems and data. It may be inferred that the Act requires management to attend to the continuity of operations; therefore, it can be said that all of the components under "Equipment Security" are relevant to SOX compliance because all of them contribute in one way or another to continuity of operations. Specifics of these relationships to the Act are given in Section A.7 of Table 1.

### **Communications and Operations Management**

All of the components in this area fall under the category of IT general controls from Paragraph 50, and many of them become specific controls to ensure the integrity of financial data when the communications or systems are involved in initiating, recording, or otherwise processing financial data (PCAOB, 2004). Change control procedures particularly stand out because such procedures are specifically mentioned in Paragraph 50 (PCAOB, 2004). Study of Table 1, Section A.8, reveals that this security area provides much of the support for data integrity controls.

### **Access Control**

Access control is the most important category for achieving SOX compliance. All components of access control, as outlined in ISO 17799, are key controls and should be the starting point

for compliance, after a risk assessment. Only careful access control can prevent or detect the recording of fraudulent or erroneous data in significant accounts. Without the ability to attribute actions to users, all of the other automated controls may be bypassed. This area of the Standard cannot be overemphasized as critical to management's success. No subordinate component or item can be overlooked in this control area, except "Duress alarm to safeguard users" under Operating System Access Control (9.5.6). For managers, Table 1, Section A.9, should be the starting point for compliance, after a risk assessment.

### **Systems Development and Maintenance**

This control category is second to access control in importance to achieving SOX compliance. This category stands as an IT general control, as outlined in Paragraph 53. However, where it is applied to financial systems and data, it is crucial in ensuring that incorrect code and data are not introduced into the financial reporting system.

One difficult task is identifying the parts of computer programs that perform input data validation. Most computer programs are documented to show function and process flow; rarely is the documentation focused on data integrity checks or other security issues.

Perhaps the only subordinate category that may not apply is the cryptographic controls category (10.3), and this is only true if cryptography is not used in ensuring the integrity of data or authenticating data or users. Section A.10 in Table 1 spells out the relevance of individual items to the Act.

### **Business Continuity Management**

In the United States, the terrorist attack on September 11, 2001, brought into sharp focus the need for business continuity planning. This need is reinforced by the reference to company-level general controls in Paragraph 53 of AS No. 2 (PCAOB, 2004). Although only a part of the continuity plan deals directly with IT, an integrated plan for the whole organization is needed to ensure an uninterrupted revenue stream. This is evident from the language of ISO 17799 that deals with business continuity planning: the component items are all of a business operations nature and almost no mention is made of any information technology (ISO, 2000, pp. 57-60). The component items listed in Section A.11 in Table 1 are all of a business operations nature.



### Compliance

Failure to comply with existing legislation may expose the firm to financial sanctions or costly litigation. Exposing the firm to this type of potential loss would be an example of managerial ineffectiveness an auditor is bound to report.

Laws and regulations concerning collection of evidence may or may not be of concern to the firm, depending on the firm's posture regarding prosecution of transgressors. There seems to be no intent in the Act to mandate prosecution of those who commit fraud, only that the fraud be detected and reported (Hardesty, 2003, p. 302<sup>7</sup>). Therefore, it appears that procedures for the collection of evidence are beyond the scope of the Act. Section A.12 in Table 1 deals with the relevance of the remainder of the compliance section to the Act.

### CONCLUSION

As can be seen from the notes on the ten categories of compliance provided in Table 1, 113 of the 124 components of the ISO Standard have direct relevance to the Sarbanes-Oxley Act of 2002. Data integrity, like information security (of which it is a part), is achieved through a set of controls, "... which could be policies, practices, procedures, organizational structures, and software functions" (ISO, 2002, p. viii). With a solid set of controls provided by ISO/IEC 17799 compliance, managers can use the PCAOB AS No. 2 to identify additional steps they may need to take to bring the firm into compliance with the Act.

Although precise needs cannot be specified without access to the documentation of a company's financial processing system, two needs emerge from our analysis: (1) the evaluation of existing controls must be much more frequent than suggested in the ISO Standard, and these results must be clearly documented and retained for auditor review; and (2) existing application documentation is likely to be inadequate to support an auditor's walkthrough.

For example, firms must develop documentation to focus on "significant accounts" and "significant transactions" that are posted to those accounts. Moreover, the documentation must support an initiation-to-financial-report walkthrough and show clearly what controls are applied where in the flow of processing. Although this type of documentation may not exist for most systems, it will offer several advantages when developed:

- The auditor's job will be easier and quicker.
- The bird's-eye view of the whole processing stream will allow management to assess the design effectiveness of the controls.
- The documentation will provide a basis for constructing realistic suites of test data.
- The documentation will provide a holistic view to support reengineering of processes, controls, or sequences for the purpose of improving security or processing efficiency.

In summary, ISO/IEC 17799 compliance, coupled with increased managerial evaluation of controls and improved documentation, can bring the firm into reasonable compliance with the mandates of the Sarbanes-Oxley Act of 2002. ▲

### References

- Hardesty, D. (2003). *Practical Guide to Corporate Governance and Accounting: Implementing the Requirements of the Sarbanes-Oxley Act*. New York, NY: Warren, Gorham & Lamont.
- ISO (International Organization for Standardization) (2000). *Information Technology — Code of Practice for Information Security Management (ISO/IEC 17799:2000(E))*. [Retrieved May 25, 2004, from <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35>.]
- PCAOB Public Company Accounting Oversight Board (2004). *Auditing Standard No. 2 — An audit of internal control over financial reporting performed in conjunction with an audit of financial statements*. New York: Author.